AMENAZAS PERSISTENTES AVANZADAS

Carbonó Carbonó Dayana
dayanacarbono@hotmail.com
Especialización Seguridad Informática
Universidad Piloto de Colombia

Abstract— *This document shows the context of the APT, the most advanced form of cyber attack, this document begins the historical context in where these modalities happened, which the interest is after shows the difference between APT and classic cattacks with the salient features of the ATP's, how to counter them and finally shows how important and relevant they have today.*

Key words—APT, attacker, attack, exfiltration, intrusion, persistence, victim.

Resumen— *Este documento da la entrada al descubrimiento de las APT's la modalidad más avanzada de ataque cibernético, en el documento se muestra el contexto histórico en que se han dado estas modalidades de ataque, los intereses por los cuales se realiza, muestra la diferencia de las APT's y los ataques comunes, continuando con las características más sobresalientes de las ATP's, la manera de contrarrestarlos y finalmente nos muestra lo importante y la relevancia que tienen en la actualidad.*

Índice de Términos— *APT, atacante, ataques, exfiltración, intrusión, persistencia, víctima.*

I. INTRODUCCIÓN

Si bien es cierto que la Seguridad de la Información ha tenido un avance en los últimos tiempos y el tema ha sido más reconocido en nuestro mundo laboral, no hay que desconocer que de la misma manera y aún más avanzado las amenazas a la información de las organizaciones (el activo más importante) han aumentado a pasos agigantados. Cada día surgen nuevas técnicas para poder acceder a sistemas y de esta manera poder lograr el fin, que son diversos tales como económicos, status, políticos, competitivos etc.

Teniendo en cuenta lo dicho anteriormente desde hace unos años atrás en el ámbito de la Seguridad de la Información ha aparecido un riesgo de Ciberseguridad de suma importancia y con efectos muy perjudiciales y al que se le debe dar importancia y tomar las medidas adecuadas para no ser víctimas.

Se trata de las APTs (Advanced Persistent Threats) en español Amenazas Persistentes Avanzadas, esta amenaza está diseñada para perdurar en el tiempo es decir como lo dice su componente, Persiste. Además se aprovecha de vulnerabilidades conocidas lo que permite que pase desapercibido y su último componente es que estas amenazas van dirigidas a un objetivo específico para realizar espionajes, objetivos empresariales, gubernamentales y/o militares para finalmente obtener información confidencial y reservada, de esta manera obtener ventajas en cada escenario.

A lo largo de este artículo nos centraremos en describir más a fondo de lo que se trata las APTs.

II. CONTEXTO

Durante toda la historia humana, quien ha contado con el conocimiento ha logrado hacer diferencia y reinar durante un tiempo, desde los antiguos romanos y su conocimiento en el manejo del agua logrando supremacía por más de VIII siglos, hasta los aliados en la Segunda Guerra Mundial con el conocimiento del radar y desciframiento de la máquina enigma, como los Estados Unidos con el conocimiento de la bomba atómica, información valiosa que hicieron de los vencedores hegemónicos hasta hoy día.

Las tendencias cambian, en relación a los objetivos, en algún momento lo fue el carbón, luego el petróleo, actualmente la economía define imperios alrededor del globo terráqueo, sin embargo, el conocimiento y el acceso a la

información será, ahora y siempre la diferencia que define ganadores o perdedores en cualquier ámbito.

Durante la Guerra Fría se conformó el máximo andamiaje del espionaje, donde al finalizar la misma todo ciudadano alemán tenía alguna relación con algún espía, maquinaria creada y mantenida durante años para lograr alguna ventaja; este esquema ha evolucionado, cambiando su escenario de desarrollo pero manteniendo el mismo esquema, ahora no contamos con líneas de comunicación a través de correos físicos y encuentros casuales con conversaciones cifradas, sino maquinarias de monitoreo desde algún lugar del mundo (un punto o varios) donde se conoce y analiza un posible *enemigo* desde su comportamiento, actividades diarias, ubicaciones geográficas, rutas de suministros, clientes más cercanos, se analiza desde las horas picos y más bajas de trabajo de una organización, información relevante para conocer desde las nuevas líneas de negocio de una empresa, patentes, como futuros aliados estratégicos para un país; para lo cual se requiere una gran inversión económica y tiempo de análisis de tanta información manejada en estos momento por todas las organizaciones, logrando deducir las situaciones que la *alta gerencia* desea conocer, conociendo esta actividad como APT's.

III. DIFERENCIA ENTRE ATAQUE CLÁSICO Y APTS

A. Ataque Clásico

Los ataques que comúnmente conocemos básicamente están divididos o compuestos de la siguiente manera:

Direccionalidad: los ataques que se realizan siempre son desde afuera hacia adentro.

Atacante: estos atacantes se caracterizan por ser aislados, los grupos son poco o nulos en la organización.

Ataques: son masivos (ciberactivismo), son conocidos y pocos discretos.

B. APT

Las APT están dividas con los mismos componentes que un ataque clásico la diferencia radica en la manera como lanzan o utilizan esos componentes.

Direccionalidad: a diferencia del ataque clásico los ataques que se realizan vienen desde adentro es decir cuando se ha realizado todo el proceso para que la amenaza se encuentre dentro del sistema o red de x organización el ataque ya está lo suficientemente maduro para ser lanzado y eso se realiza desde adentro en eso radica la diferencia con el clásico.

Atacante: son personas o grupos estrictamente organizados hasta el punto de tener horarios de trabajo como lo realiza un trabajador normal adicional a esto el objetivo que quieren cumplir es específico y claro.

Ataques: estos se caracterizan por ser desconocidos, sigilosos y persistentes.

Lo que se pretende obtener con la APT finalmente es Ciberespionaje, el Ciberespionaje es básicamente el espionaje tradicional (adquirir información importante para la organización y para el atacante) con un ingrediente adicional como lo es la tecnología, es por eso que la manera como operan es sigilosamente y persistente ya que la información que se requiere no es solo por un momento, es analizar y descubrir los secretos de la organización para ir un paso adelante.

IV. FORMA DE OPERAR

Las APT's cuenta con una manera de proceder sigiloso, iniciando con un *Reconocimiento* identificando y analizando la víctima, su esquema de internet, el uso de las redes sociales, siendo fundamental conocer el alcance e importancia que pueda tener la posible víctima, de lo contrario no tendría sentido realizar una gran inversión sin un objetivo importante.

Intrusión: en esta fase se debe establecer la manera de entrar a la organización, la cual puede ser unilateral o multidireccional, a través de Dropper o algún mecanismo que logre la intrusión a la organización.

Persistencia: luego de establecida la intrusión a una o diferentes máquinas de la organización, claramente definidas, se procede a permanecer en ellas sin generar alarma alguna, este proceso puede

durar años o días, dependiendo del resultado que arroje el mismo.

Exfiltración: logrando la permanencia en la organización afectada, se debe extraer la información, que se considere puede ser relevante o importante para los objetivos establecidos en la primera fase. A continuación se muestra un resumen de la forma de operar de las APT's.

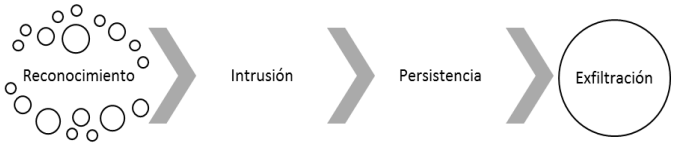

Figura 1. Forma de Operar. Fuente: El autor.

V. MÉTODO DE INFECCIÓN Y ATAQUE

A. Ingeniería Social

Esta técnica es la más utilizada para adquirir información de la víctima y de esta manera perpetuar el ataque, aunque ésta a simple vista es inofensiva es una de las más peligrosa y más efectiva teniendo en cuenta que se realizan con artimañas y va dirigido al eslabón más débil de la cadena es decir a las personas.

B. Bring Your Own Device (BYOD)

Este método de "Trae tu propio dispositivo" utilizado por varias empresas puede ser contraproducente ya que por este mecanismo pueden acceder dispositivos no protegidos ni controlados, además se puede extraviar o ser robado y el atacante puede aprovecharse de la situación.

C. Vulnerabilidades

En los sistemas de Información existen vulnerabilidades que si llegasen a ser potencialmente graves, el atacante puede explotarla e ingresar a la organización y realizar el ataque [1].

D. Phishing dirigido

A diferencia del Phishing habitual que es suplantar una página web bancaria para robo de credenciales bancarias y es lanzado a todas las personas sin importar si realmente son clientes de un banco especifico, el Phishing utilizado en APTs es para robar credenciales de las personas que trabajan en las organizaciones o empresas objetivo, esto quiere decir entonces que son personas que ya han identificado con anterioridad lo que hace que los mensajes y la suplantación no sea indiscriminado.

E. Distracciones

Como se ha mencionado anteriormente una de las características de las APTs es la persistencia, es por ellos que los atacantes realizan la técnica de las distracciones que consiste en enviar ataques a la red para que las personas responsables de la red se entretengan mitigando o anulando el evento del riesgo mientras tanto ellos ingresan el malware sin dejar rastros en los logs y así poder ingresar sin ningún inconveniente, la idea de este ataque es no ser descubierto así que lo que realizan lo hacen de manera sigilosa y con la mayor paciencia que se pueda.

VI. EJEMPLOS DE APTS

A lo largo del tiempo se han realizado ataques de APTs que han revolucionado y han catalogado como altamente peligrosos, a continuación se nombran algunos:

A. Stuxnet

Esta APT se descubrió en julio de 2010. Su objetivo fue infectar de manera indiscriminada a sistemas operativos Windows y afectar únicamente a sistemas SCADA[1]. Esta APT es considerada un gusano ya que tiene la capacidad o característica de auto-distribuirse, a continuación se muestra la manera de operar:

Infección: se utilizó una vulnerabilidad de auto-ejecución de archivos en dispositivos de almacenamiento USB. Hasta el momento se desconoce cuál fue la técnica utilizada para ejecutarse.

Propagación: Al ya estar infectado un equipo, el siguiente paso es propagarse a través de la red a otros sistemas (SCADA), esta vez utilizando dos vulnerabilidades 0-day, una en la cola de impresión

[1] SCADA (Supervisory Control And Data Acquisition) son sistemas, como su propio nombre indica, para la adquisición, control y supervisión de datos de procesos industriales. Con ellos se pueden controlar desde las revoluciones de un motor hasta un sistema de temperatura de un frigorífico industrial.

y otra en el servidor donde se comparten archivos. En el equipo que fue infectado al inicio, se utilizaron también dos vulnerabilidades 0-day esto con el propósito de escalar privilegios y llegar a ser administrador dentro de la red.

Esta amenaza se aprovechó de una vulnerabilidad que es muy repetida en la administración de las redes y es dejar las contraseñas por defecto de los sistemas, aunque se habla mucho de ella para que se pueda corregir en pleno 2015 aún existen administradores que no toman conciencia y al realizar pruebas de penetración especialistas aún se encuentran con esta vulnerabilidad.

Esta amenaza considerada altamente peligrosa era capaz de actualizarse de esta manera podía estar oculta o incluía nuevas funcionalidades para poder continuar con su objetivo.

La amenaza Stuxnet fue encontrada en sistemas e infraestructuras de varios países entre ellos Indonesia, India, Irán y China el objetivo principal según los medios de comunicación eran las centrales nucleares iraníes, lo que se pone al descubierto es que los atacantes estaban examinando potencias mundiales no era cualquier objetivo. Una muestra que estas amenazas son debidamente organizadas y planeadas de manera cautelosa es que duraron muchos años en los sistemas antes de ser descubierta [3].

B. *TheFlame*

Para esta APT se realizó su descubrimiento en mayo de 2012, la manera de operar de esta amenaza es la siguiente:

Infección: su método de infección inicialmente es a través de dispositivos de almacenamiento USB como lo realizaba Stuxnet.

Propagación: esta amenaza se replicaba en la red interna haciendo uso del ataque MitM[2] también conocido como "hombre en el medio", simulando ser una actualización de Windows.

Cuando un equipo era infectado por esta amenaza realizaba las veces de un proxy así de esta manera cuando otro equipo perteneciente a la red se actualizaba, preguntaba si existía un proxy y el equipo infectado se ofrecía a serlo con esto los atacantes tenían el control ya que redirigían la petición a un servidor en su poder y envían una actualización con la amenaza TheFlame camuflada.

The Flame es modular esto quiere decir que es creada para grabar audio, hacer capturas de pantalla, pulsaciones de teclado, escanear el tráfico de red, grabar conversaciones de Skype, controlar el bluetooth del equipo infectado.

Otra característica del TheFlame es que es adaptativo lo que permite que cambie su comportamiento dependiendo el antivirus instalado en la máquina infectada de esta manera lo hace más difícil de detectar, además los equipos infectados eran considerados "Zombies" ya que los atacantes tenían la posibilidad de darles órdenes y estas máquinas las ejecutaban.

Los países Oriente Medio fueron los más afectados por esta amenaza [1].

Figura 2. Técnicas comunes usadas por APT. Tomada de http://observatorio.inteco.es

VII. CONTRARRESTRAR

Las APT's pueden presentar comportamientos muy particulares, razón por la cual en un proceso de Gestión de Incidentes no se logran identificar a simple vista, si nuestra entidad o empresa puede ser posible objetivo por nuestra naturaleza, debemos incluir actividades adicionales a una Gestión de Indecentes convencional, para lo cual se recomiendan las siguientes acciones:

A. *Detección de usos indebidos*

A través de las listas negras se puede identificar, detectar y neutralizar al posible invasor, sin embargo, en esta instancia a diferencia de un

[2] MitM (Man-in-the-Middle) es un tipo de ataque en el que el atacante es capaz de situarse entre el cliente y un servidor legítimo, pudiendo leer, modificar y/o eliminar cierta información que fluya entres estos.

incidente tradicional, no debemos neutralizar inmediatamente (ya lleva tiempo en nuestra organización), en esta parte es importante conocer la mayor cantidad posible de información sobre nuestro posible invasor.

B. Comunicación periódica

Debido a la naturaleza de las APT's siempre se contará con comunicación periódica en la necesidad de enviar información (este es el objetivo) por tal razón, debemos analizar posibles comunicaciones externas, bajas, con criterios similares, horas, fechas, conjunto de ambas; identificar malware no avanzados, tener presente la comunicación en horarios laborales.

C. Anomalías estadísticas

Al igual que un análisis de posibles anomalías en nuestros sistemas, debemos incluir, campos anómalos (estadísticamente) en la navegación: Content-Type, método HTTP, código HTTP, TLD, análisis de frecuencias o distribuciones, tener presente que el malware más avanzado no generará estas anomalías e identificar detecciones triviales.

D. Exfiltración satelital

Continuando con el análisis de exfiltraciones, debemos incluir al análisis las conexiones extremadamente lentas, tamaño pequeño vs duración elevada (técnica utilizada para dificultar el rastreo del origen), apoyarse en detección de anomalías estadísticas y multivariable [2].

Con estos pasos es posible mitigar las posibles ATP's, sin embargo, la actividad debe ser constante y cautelosa, en cuanto el posible atacante identifique nuestro conocimiento de él, hará un borrado masivo y saldrá librado de nuestro conocimiento, más adelante seremos victimas de nuevo. En esta época toda organización con información importante es blanco de ATP's en la mayoría de los casos seguramente son víctimas, la cautela y paciencia deben ser nuestra mayor arma para lograr mitigar levemente esta nueva amenaza.

VIII. CONCLUSIONES

Las Amenazas Persistentes Avanzadas es un tema al que las empresas y los gobiernos deben darle la importancia que merece, teniendo en cuenta la manera organizada de cómo operan los grupos de atacantes que se dedican a realizar este ataque APTs.

No se debe caer en el error de confundir las APTs con ataques clásicos, teniendo en cuenta que aunque tengan características similares la manera de operar de las dos son diferentes, las APTs evolucionan haciendo uso del factor tiempo y paciencia por parte de los grupos organizados de atacantes.

En determinado caso que se descubra en una organización x una APT, hay que tener claro que ese atacante o el grupo de atacante volverán, lo que se ha eliminado o erradicado es un malware no los intereses de los atacantes, teniendo en cuenta lo anterior se deben plantear estrategias para responder a un nuevo ataque de ese tipo.

Una APT no es un malware, no debe tratarse como una simple infección ya que vas más allá el considerarse de esa manera sería un error grave.

En este tipo de ataque y en todos los ataques, el eslabón más débil de la cadena es el recurso humano, por tal motivo en cada estrategia emprendida se debe considerar sensibilizar a las personas en cuanto a estos temas.

Es de vital importancia que los profesionales de Seguridad Informática o Seguridad de la Información estemos actualizados en cuanto a los temas que nos competen como especialistas ya que cada día aparecen ataques nuevos y mejorados, esto quiere decir que las personas que están al otro lado del camino es decir los atacantes no se detienen por conseguir sus objetivos, es responsabilidad de cada especialista seguir investigando y empapándose de los temas y así poder estar al frente de nuestra área (seguridad de la Información) en las empresas como los profesionales que somos.

REFERENCIAS

[1] Instituto Nacional de Tecnologías de la Comunicación "Advanced Persistent Threats (APTs)", disponible en http://inteco.or.cr/esp/

[2] Antonio Villalón "Como ganar la batalla contra las APTs", disponible en http://www.s2grupo.co/
[3] The New York Times "Obama Order Sped Up Wave of Cyberattacks Against Iran", disponible en http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Dayana Carbonó Carbonó
Ingeniera de Sistemas Universidad Incca de Colombia
Estudiante Especialización Seguridad Informática Universidad Piloto de Colombia.